

IN THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF DELAWARE

~~SEALED~~

UNSEALED  
9/30/14  
KJL

UNITED STATES OF AMERICA

v.

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampupstechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic,"

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

Defendants.

CRIMINAL NO. 13-

78-UNA

Count 1: Conspiracy  
(18 U.S.C. § 371)

Count 2: Conspiracy to Commit Wire Fraud  
(18 U.S.C. §§ 1343 and 1349)

Counts 3-6: Wire Fraud  
(18 U.S.C. § 1343)

Count 7: Conspiracy to Commit  
Theft of Trade Secrets  
(18 U.S.C. §§ 1832(a)(1), (a)(2), (a)(3), (a)(5))

Counts 8-10: Unauthorized Computer Access  
(18 U.S.C. §§ 1030(a)(2)(C) & 2)

Counts 11-12: Criminal Copyright Infringement  
(18 U.S.C. § 2319(d)(2); 17 U.S.C. § 506(a)(1)(C) & 2)

Count 13: Conspiracy to Commit Mail Fraud  
(18 U.S.C. §§ 1341 and 1349)

Count 14: Attempted Mail Fraud  
(18 U.S.C. §§ 1341 and 1349)

Count 15: Conspiracy to Commit Identity Theft  
(18 U.S.C. § 1028(f))

Count 16: Aggravated Identity Theft  
(18 U.S.C. § 1028A & 2)

Forfeiture Notice

Filed Under Seal

**INDICTMENT**

The Grand Jury for the District of Delaware charges that:

**COUNT 1**  
**(Conspiracy)**  
**18 U.S.C. § 371**

1. At all times material to this Indictment:

**The Defendants**

- a. Defendant NATHAN LEROUX, a/k/a "natelx," a/k/a "animefre4k," a/k/a "confettimancer," a/k/a "void mage," a/k/a "Durango," a/k/a "Cthulhu," ("LEROUX") resided in or near Bowie, Maryland.
- b. Defendant SANADODEH NESHEIWAT, a/k/a "rampuptechie," a/k/a "Soniciso," a/k/a "Sonic" ("NESHEIWAT") resided in or near Washington, New Jersey.
- c. Defendant DAVID POKORA, a/k/a "Xenomega 9," a/k/a "Xenon7," a/k/a "Xenomega," ("POKORA") resided in or near Mississauga, Ontario, Canada.

**Co-conspirators**

- d. C.W., a/k/a "Gamerfreak," a co-conspirator who is not charged herein, resided in or near Morganton, North Carolina.
- e. [REDACTED] a minor and co-conspirator who is not charged herein, a/k/a "savingthefrog," a/k/a "alliyainwonderland," a/k/a "ohaiithar," a/k/a "SuperDae," a/k/a "Dae," resided in or near Perth, Western Australia, Australia.

**Methods of Hacking Utilized by Defendants**

- f. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data in computer databases.
- g. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.
- h. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

- i. "Malware" was malicious computer software programmed to gain unauthorized access to computers; to evade detection of intrusions by anti-virus programs and other security features running on those computers; and to identify, store, and export information from hacked computers, including information such as Copyrighted Works, Works Being Prepared for Commercial Distribution, user names and passwords ("Log-In Credentials"), means of identification ("Personal Data"), authentication keys used to protect copyrighted works ("Authentication Keys"), internal corporate documents, including attorney-client communications ("Corporate Documents"), credit and debit card numbers and corresponding personal identification information of cardholders ("Card Data").

#### **The Victims of Computer Hacking**

- j. Microsoft Corporation ("Microsoft") was a provider of computer software, hardware, video games, game engine technology, online gaming platforms, and related products and services. Microsoft was headquartered in Redmond, Washington. Microsoft is the developer, manufacturer and intellectual property rights holder of the Xbox gaming console (hereinafter "Xbox"). The latest version of the Xbox gaming console -- which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," and which has not yet been released for sale to consumers -- is a computer system and multimedia entertainment and telecommunications hub that allows users not only to play computer games, but also to watch television and movies and to access the Internet. Microsoft has spent millions of dollars developing the Xbox gaming consoles, including Xbox One. Microsoft's Xbox-related revenues for 2011 and 2012 exceeded \$8 billion per year.
  - i. Microsoft is also the copyright holder for the underlying technology employed in the "Gears of War 3" Xbox game, which was released to the

public on September 20, 2011. "Gears of War 3" sold more than 3 million copies in its first week of release, at an initial Manufacturer's Suggested Retail Price of \$59.99.

- ii. Microsoft operated a "Game Development Network Portal" ("GDNP"), which was a private computer network allowing prospective developers of games for Microsoft's Xbox and other gaming platforms to access, through an authentication system, the pre-release Xbox "Durango" operating system development tools and software. Microsoft controlled access to the GDNP by, among other methods, imposing licensing requirements, non-disclosure agreements and other restrictions and requiring authorized users to be registered with Microsoft. Microsoft also administered separate access enclaves for more-restricted data on GDNP.
- iii. Microsoft also provided developers with access to a software platform known as "PartnerNet" to refine video game creation. Microsoft controlled access to PartnerNet by, among other methods, imposing licensing requirements, non-disclosure agreements and other restrictions and providing authorized network users with an "Xbox Development Kit" ("XDK"), which are non-retail computers used to access PartnerNet.
- iv. Beginning in or about January 2011, Microsoft was the victim of incidents of unauthorized access to its computer networks, including GDNP's protected computer network, which resulted in the theft of Log-In Credentials, Trade Secrets, and Intellectual Property relating to its Xbox gaming system.

- k. Epic Games, Inc. ("Epic") was a developer of computer games, and cross-platform game engine technology, including software used in electronic gaming consoles such as Microsoft's Xbox gaming system. Epic was headquartered in

Cary, North Carolina. Beginning in or about January 2011, Epic was the victim of a SQL Injection Attack and other incidents of unauthorized access to Epic's protected computer network that resulted in the theft of Intellectual Property from its network, including unreleased software, source code, and middleware from the software title "Gears of War 3," which Epic developed exclusively for the Microsoft Xbox gaming system. Epic holds certain copyrights and trademarks related to the "Gears of War 3" game.

- l. Valve Corporation ("Valve") was a developer of computer games, game engine technology, and online gaming platforms, and the operator of the "Steam" online gaming forum and merchandise store. Valve was headquartered in Bellevue, Washington. Beginning in or about September 2011, Valve was the victim of a SQL injection attack and other incidents of unauthorized access to Valve's protected computer network that resulted in the theft of Intellectual Property and Personal Data from its network, including the theft of Log-In Credentials for Valve employees.
- m. Activision Blizzard Inc. ("Activision") was a publisher of interactive online gaming software for personal computers, consoles, handheld and mobile devices. Activision was headquartered in Santa Monica, California. Activision was the publisher of, and holds various copyrights and trademarks relating to, the video game "Call of Duty: Modern Warfare 3," which generated approximately \$1 billion in sales in the first 16 days of its release on November 8, 2011.
- n. Zombie Studios ("Zombie") was a developer of computer games and helicopter simulation applications for the United States Department of the Army. Zombie was headquartered in Seattle, Washington. Beginning in or around July 2012, Zombie was the victim of unauthorized access to Zombie's protected computer

network that resulted in the theft of Intellectual Property and Personal Data from its network.

- o. The United States Department of the Army is one of three military departments within the United States Department of Defense. Beginning in or about October 2012, the United States Department of the Army was the victim of unauthorized access to and trespass into one of its protected computer networks that resulted in the theft of confidential data valued at more than \$5,000.

### THE CONSPIRACY

2. Between in or about January 2011 and in or about April 2013, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natebx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

did knowingly and intentionally conspire and agree among themselves and with others known and unknown to the grand jury, including [REDACTED] C.W., to commit offenses against the United States, namely:

- a. Fraud and Related Activity in Connection with Computers by intentionally accessing a protected computer used in or affecting interstate or foreign

commerce without authorization, and exceeding authorized access to a protected computer, and thereby obtaining information from that computer, namely Log-In Credentials, Personal Data, Authentication Keys, Corporate Documents, Card Data, and Intellectual Property, for the purpose of commercial advantage and private financial gain, and the value of that information exceeds \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i) and (iii);

- b. Fraud and Related Activity in Connection with Computers by intentionally accessing a protected computer used in or affecting interstate and foreign commerce and exclusively for the use of the United States Government, and exceeding authorized access to a protected computer, and thereby obtaining information from any department or agency of the United States, for the purposes of commercial advantage and private financial gain and the value of the information obtained exceeds \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (C) and (c)(2)(B)(i) and (iii);
- c. Criminal Copyright Infringement by the distribution, for the purpose of commercial advantage and private financial gain, of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, where the defendants knew or should have known that the work was intended for commercial distribution, in violation of Title 17, United States Code, Section 506(a)(1)(C), and Title 18, United States Code, Section 2319(d)(2).

**OBJECT OF THE CONSPIRACY**

3. It was the object of the conspiracy for LEROUX, NESHEIWAT, POKORA, [REDACTED] and others to hack into the computer networks of Microsoft, Epic, Valve, Activision, Zombie, and the United States Department of the Army (collectively "the Victims") to steal and then to use, share, and sell Network Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution, and to otherwise profit from their unauthorized access.

**MANNER AND MEANS OF THE CONSPIRACY**

4. The manner and means by which LEROUX, NESHEIWAT, POKORA, [REDACTED] and others sought to accomplish the conspiracy included, among other things, the following:

**Scouting Potential Victims**

- a. It was part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would identify potential victims by, among other methods, visiting the websites of potential victims, as well as related companies, to identify potential vulnerabilities of their information systems, and conducting research to determine whether their information systems had already been breached.
- b. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would scan the "ports," or information portals of computers belonging to potential victims, to locate network weak points.
- c. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would visit websites where another hacker had posted

legitimate Log-In Credentials for potential victims, and would copy those Log-In Credentials and save them for subsequent use.

**Launching the Attacks – The Hacking Platforms**

- d. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would lease, control, and use Internet-connected computers in New Jersey, California, Canada, Utah, Texas, the Netherlands, Hong Kong, Australia, the United Kingdom, and elsewhere (collectively, “the Hacking Platforms”) to: (1) store malware; (2) stage attacks on the Victims’ networks; and (3) receive, store and share stolen Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution.
- e. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would provide each other and others with unauthorized access to the Victims’ networks and would locate, store, and transmit Network Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims’ networks.
- f. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would hack into the Victims’ networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things, Network Log-In Credentials, Personal Data, Authentication

Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks.

- g. It was further part of the conspiracy that if LEROUX, NESHEIWAT, POKORA, and [REDACTED] obtained Log-In Credentials that were encrypted, POKORA would defeat the encryption using software programs such as "Passwords Pro" and "Password Recovery Magic," so that LEROUX, NESHEIWAT, POKORA, and [REDACTED] could subsequently use the decrypted Log-In Credentials to access the Victims' networks.

**Executing the Attacks – Obtaining Confidential and Proprietary Information and Intellectual Property from the Victims**

- h. It was further part of the conspiracy that once they hacked into the computer networks, LEROUX, NESHEIWAT, POKORA and [REDACTED] would conduct network reconnaissance to find and to steal Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks.
- i. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA and [REDACTED] would use an unauthorized Comcast cable modem belonging to NESHEIWAT and physically located in New Jersey to connect to the Internet to steal Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. The conspiracy used the unauthorized Comcast cable modem

because its members believed that the modem could not be traced to the conspiracy, and further to avoid the limitations on Internet bandwidth usage that Internet Service Providers apply to legitimate users of their networks.

- j. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would communicate via the computer program Skype, which allowed them to use their Internet connections to talk to and advise each other in real time regarding how to navigate the Victims' networks and to locate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between computers connected to the Internet from, among other places, Ontario, Canada, Delaware, New Jersey, Maryland, and Australia.
- k. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] and others would use the computer program TeamViewer to remotely view other computer desktops in real time, and to allow them to communicate about their unauthorized access of the Victims' networks and the location of Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between computers connected to the

Internet from, among other places, Ontario, Canada, Delaware, New Jersey, Maryland, and Australia.

- l. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would communicate via the computer program AOL Instant Messenger ("AIM"), which allowed them to use their Internet connections to exchange messages with each other in real time; to share files; to provide access to websites they controlled; and to direct each other on how to navigate the Victims' networks and locate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks. By doing so, their electronic communications traveled between computers connected to the Internet from, among other places, Ontario, Canada, Delaware, New Jersey, Maryland, and Australia.
- iii. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] and others would use computer servers located in various states and countries, including Utah, Texas, the United Kingdom, and Canada to store, receive and disseminate Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution stolen from the Victims' networks.

**Concealing the Attacks**

- n. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would conceal their hacking into the Victims' networks by, among other things, conducting their hacking via Virtual Private Networks, including but not limited to computer programs that used encryption to protect communications transmitted via the Internet.
- o. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would conceal their hacking into the Victims' networks by, among other things, disguising their true Internet Protocol addresses through the use of "proxies," or intermediary computers.
- p. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would conceal their theft of Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution from the Victims' networks by encrypting the contents of their own computers and digital media with TrueCrypt and other encryption software.
- q. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would conceal their activities within the Victims' computer networks by utilizing Log-In Credentials, Personal Identifiers, and Authentication Keys of other individuals to steal data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and

Works Being Prepared for Commercial Distribution from the Victims' computer networks.

- r. Defendants undertook such efforts at concealment to attempt to avoid detection by the Victims and law enforcement agencies. During an August 21, 2011 electronic communication session via the Internet, for instance, POKORA stated:

Have you been listening to the shit that I've done this past month?

I have shit to the U.S. military. I have shit to the Australian Dept. of Defense.

....

I have every single big company: Intel, AMD, Nvidia, any game company you could name, Google, Microsoft, Disney, Warner Brothers, everything.

...

It's not like I'm trying to prove a point, but I'm just saying, if they notice any of this, eventually they're going to come looking for me.

**Profiting from the Attacks**

- s. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] attempted to sell Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution stolen from the Victims' computer networks.
- t. During a chat session on or about October 2, 2011 between POKORA and [REDACTED] for example, POKORA wrote, in reference to ongoing computer

intrusions into the Victims' computer networks: "if we do this right, we will make a million dollars each." POKORA also stated in a Skype audio call, "I don't think you understand the plan that I had. I've already compromised a fuckton of Paypals from those databases we have. Not that I logged into them, but I've compromised enough that we could have already sold them for Bitcoins which would have been untraceable if we did it right. It could have already been easily an easy 50 grand."

- u. During an October 2, 2011 hacking session, POKORA and his co-conspirators initiated a Remote Desktop Protocol connection to Epic's computer network through an intermediary network node controlled by [REDACTED] POKORA and his co-conspirators, using computers located in Delaware, Australia, Canada, New Jersey and Maryland, logged into Epic's webmail server with the Log-In Credentials of an Epic employee who was assigned to respond to known intrusions into Epic's computer network. While POKORA and others viewed the Epic employee's e-mail through TeamViewer, [REDACTED] wrote, using AIM:

Look at the e-mails between them about me.  
Haha.  
But fuck, I don't even get anything fun out of it anymore.  
Its degrading.  
Making money out of it.  
Fuck.

- v. On or about November 3, 2011, POKORA instructed Person A to obtain a "wish list" of pre-release intellectual property from online alias "XBOXDEVGUY." POKORA had previously negotiated with XBOXDEVGUY to hack into companies to obtain software for compensation.

- w. POKORA, [REDACTED] and other co-conspirators used online merchants to purchase Apple computer products with the proceeds of their criminal activity.
- x. In or about August 2012, LEROUX and his co-conspirators gained unauthorized access to Microsoft computer networks, from which they downloaded Trade Secrets and Copyrighted Works owned by Microsoft. LEROUX used Microsoft's Trade Secrets, including internal design and technical specifications and pre-release operating system software code, to build a counterfeit, next-generation Microsoft Xbox gaming console, which he and other co-conspirators sold online.
- y. In or about August 2012, [REDACTED] used the personally-identifying information of two individuals, C.L. and M.L., including name, social security number, date of birth, and address, to which he gained access in the course of the above-referenced computer intrusions, to fraudulently open financial accounts in the names of the two victims.

#### OVERT ACTS

5. In furtherance of the conspiracy, the following overt acts, among others, were committed in the District of Delaware and elsewhere:

##### Epic Computer Network

- a. In or about January 2011, POKORA learned that C.W., an unindicted co-conspirator, had conducted a SQL Injection Attack against Epic, and revealed Log-In Credentials for Epic's protected computer network.
- b. In or about January 2011, POKORA used legitimate Epic Log-In Credentials to gain unauthorized access to Epic's computer network, and to copy and

download Epic's Copyrighted Works and Works Being Prepared for Commercial Distribution, including the game "Gears of War 3," to a computer controlled by POKORA and hosted on a server in Utah. "Gears of War 3" was developed by Epic and had not yet been commercially released. The copyrights and trademarks to "Gears of War 3," which was commercially released on September 20, 2011, are held by Epic and Microsoft.

- c. On or about January 12, 2011, [REDACTED], an unindicted co-conspirator, transmitted from Australia, via the Internet, a request for technical support to Bluehost.com, a company located in Houston, Texas, that hosted a website controlled by [REDACTED] and that he and his co-conspirators used to store and disseminate stolen Log-In Credentials, Personal Data, Authentication Keys, Card Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution. [REDACTED] complained that file transfer through his website was occurring too slowly, and provided Bluehost.com with Internet-routing data showing that [REDACTED] was connecting to Epic's computer network.
- d. In or about June 2011, [REDACTED] used legitimate Epic Log-In Credentials to gain unauthorized access to Epic's network, and copied a legal document belonging to Epic and marked "Attorney-Client Privileged" to a computer controlled by [REDACTED]
- e. In or about June 2011, POKORA told the co-conspirators and others known and unknown to the grand jury via an electronic communication over Skype and transmitted to computers connected to the Internet from, among other

places, Delaware, New Jersey, Maryland and Canada: "Somebody leaked Epic Games' database. I already had it before that guy but someone else leaked it. Then they tightened their security, but the funny thing is I still have root access to all their computers, cause I signed in yesterday. I gave them one that I stole from Epic."

- f. On or about June 2011, NESHEIWAT unlawfully downloaded from Epic's computer network certain Copyrighted Works and Works Being Prepared For Commercial Distribution, including "Gears of War 3," which was developed by Epic and had not yet been commercially released. The copyrights and trademarks to "Gears of War 3," which was commercially released on September 20, 2011, are held by Epic and Microsoft.
- g. On or about July 15, 2011, NESHEIWAT sent POKORA a package labeled "Wedding Videos," which included Blu-Ray discs containing Copyrighted Works and Works Being Prepared for Commercial Distribution, including "Gears of War 3" gaming software.
- h. On or about July 8, 2011, the co-conspirators provided Person A, who was connected to the Internet from Delaware, with access to a website controlled by POKORA. The co-conspirators permitted Person A to download approximately 39 files from POKORA's website. These files contained Copyrighted Works and Works Being Prepared for Commercial Distribution, including Epic and Microsoft's "Gears of War 3" gaming software.
- i. On or about July 19, 2011, via an electronic communication over Skype and transmitted to computers connected to the Internet from, among other places,

Delaware, New Jersey, Maryland and Canada, POKORA solicited the assistance of his co-conspirators and Person A in installing encryption software on his hard drives. During the conversation, POKORA stated: "I need your help. I'm going to get arrested." POKORA subsequently stated: "I need to encrypt some hard drives." A co-conspirator stated: "If you encrypt it right, they're not going to find anything."

- j. On or about July 20, 2011, via an electronic communication over Skype and transmitted to computers connected to the Internet from, among other places, Delaware, New Jersey, Maryland and Canada, POKORA offered to provide the co-conspirators and Person A with access to "Gears of War 3." Referring to possible interactions with law enforcement if such activity was discovered, POKORA stated: "If we ever go disappearing, just, you know, upload it to the Internet and say fuck you Epic, if you know, they ever go after us."
- k. On or about September 28, 2011, via electronic communications transmitted to computers connected to the Internet from, among other places, Delaware, New Jersey, Maryland and Canada, POKORA, his co-conspirators and Person A utilized TeamViewer software to jointly and remotely access a computer controlled by POKORA. This computer contained multiple databases within a "Hacking" folder, labeled in a manner consistent with the Victims' names, including: Epic Games (*i.e.*, "epicgames\_user\_db\_cracked") and Valve Corp. (*i.e.*, "steam\_valve\_accs.html"). POKORA provided Person A with access to these databases, which contained compromised means of identification for over 200 individual victim accounts, including fields such as

username, password, and e-mail address. POKORA also provided access to usernames, passwords, encrypted passwords or "password hashes," and e-mail addresses, for approximately 47 additional accounts.

- l. On or about October 2, 2011, via electronic communications transmitted to computers connected to the Internet from, among other places, Delaware, New Jersey, Maryland, Australia and Canada, POKORA, his co-conspirators and Person A initiated a Remote Desktop Protocol connection to Epic's computer network through an intermediary network node controlled by [REDACTED] POKORA and the others logged into Epic's webmail server with the Log-In Credentials of an Epic employee who was assigned to respond to known intrusions into Epic's computer network. POKORA and the others accessed an Epic e-mail account and visually reviewed approximately 35 Authentication Keys. POKORA then directed his co-conspirators and Person A to a "Pastebin.com" website, where the same Epic e-mail account and proprietary software keys had been posted.
- m. On or about March 2012, [REDACTED] transferred a partial software build of "Gears of War 3" via the Internet to an individual using the alias "Xboxdevguy."
- n. In multiple Skype chats occurring in May and July 2012, via computers connected to the Internet from Delaware and Australia, [REDACTED] provided Person A with the credit card information for an Epic Games corporate credit card issued to Epic employee S.S., including the card number, cardholder name, expiration date, and card brand.

**Valve Computer Network**

- o. On or about September 28, 2011, POKORA obtained legitimate Log-In Credentials for Valve's computer network, including those of Valve Information Technology employees.
- p. These Log-In Credentials were stored by POKORA in multiple databases that contained usernames, passwords, and e-mail addresses for numerous Valve employees. POKORA saved these database files to a computer under his control within a file directory named  
"/Hacking/Databases/Importantdbs/Cracked." POKORA allowed Person A, who connected to the Internet from Delaware, to view these database files.
- q. Utilizing TeamViewer, Skype audio calls, and AIM, via computers connected to the Internet from, among other places, Delaware, New Jersey, Maryland, Australia and Canada, POKORA, his co-conspirators and Person A used legitimate Log-In Credentials to gain unauthorized access to Valve's network, and distributed a file named "MW3\_MP\_BETA\_1.rar." This file contained a computer game called "Call of Duty: Modern Warfare 3," which was being prepared for commercial release by Activision Blizzard, Inc., the holder of various trademarks and copyrights relating to the game. "Call of Duty: Modern Warfare 3" was commercially released on November 8, 2011.
- r. After obtaining "Call of Duty: Modern Warfare 3," POKORA used AIM to transmit to [REDACTED] a link allowing him to download "Call of Duty: Modern Warfare 3."

- s. On or about September 27, 2011, POKORA provided Person A, who was connected to the Internet from Delaware, with a link to a domain controlled by [REDACTED] Person A downloaded "MW3\_MP\_BETA\_1.rar" from this website.
- t. During the group's theft of "Call of Duty: Modern Warfare 3" from Valve, POKORA and his co-conspirators made the following statements:
  - i. When discussing the "Modern Warfare 3" file download, a co-conspirator stated: "you don't get those unless you're Valve," to which POKORA responded: "well; unless you're us."
  - ii. POKORA additionally stated: "yeah, let's get arrested."
  - iii. POKORA characterized his access to the software with the following statements:
    - 1. "I'm going to setup the laptop so it's ready to steal shit."
    - 2. "first I'm going to have to grab it off the [Valve] FTP."
    - 3. "then I'm going to be looking at files actually on the network."
- u. POKORA used an Internet-connected computer controlled by [REDACTED] to store the stolen copy of "Call of Duty: Modern Warfare 3."
- v. Also located on the Internet-connected computer controlled by [REDACTED] was a file named "steamfkn.png," which contained a screenshot of the administrator interface for Valve's "Steam" website as an unauthorized download of a file named "vbulletin.sql" was being conducted from Valve's network. Over the screenshot was the text: "Ruddified fkn0wned steam." Billing and account records show that [REDACTED] was the owner of the Internet domain "www.ruddified.com."

**Zombie Studios Computer Network and U.S. Army Virtual Private Network**

- w. On or about May 14, 2012, during an online communications session, [REDACTED] and Person A, who was connected to the Internet from Delaware, discussed computer intrusions into Zombie Studios. [REDACTED] stated, in part:
- Time to see if I can connect to Zombie Studios still  
pull some military shit  
....  
They have a tunnel to the US Army  
...  
The most I did was connect to their side of the P4. . . .
- x. On or about July 29, 2012, via computers connected to the Internet from, among other places, Delaware, Maryland, Australia and Canada, [REDACTED], LEROUX and others, including Person A, utilized TeamViewer software to intrude into the computer network of Zombie Studios.
- y. During this intrusion, [REDACTED] accessed pre-release software and software builds for gaming software being developed by Zombie Studios, as well as personally identifying information of Zombie Studios' employees. [REDACTED] transmitted the means of identification, including the name, social security number, home address, and tax documents, of "C.L.," a Zombie Studios employee, to Person A in Delaware. After gaining access to C.L.'s Personal Data, [REDACTED] subsequently submitted credit card applications in the names of C.L. and M.L. for limits of \$15,000 and \$10,000. [REDACTED] additionally attempted to open a "Lendingclub.com" account in the name of C.L. for

approximately \$20,000. [REDACTED] accessed these accounts online and provided a Delaware mailing address associated with Person A to defeat financial institution anti-fraud countermeasures.

- z. Person A subsequently received credit account activation notices in the names of C.L. and M.L. via United States Mail, at a Delaware address.
- aa. On or about July 31, 2012, via computers connected to the Internet from, among other places, Delaware, Maryland, Australia and Canada, [REDACTED], LEROUX and others, including Person A, utilized TeamViewer software to participate in a Remote Desktop Protocol intrusion into the computer network of Zombie Studios.
- bb. During this intrusion, [REDACTED] and his co-conspirators accessed Works Being Prepared for Commercial Distribution and pre-release software builds for gaming software being developed by Zombie Studios through computers and network assets controlled by Zombie Studios and its employees. [REDACTED] and his co-conspirators accessed approximately 18 computers, websites, accounts, and/or network shares using unauthorized credentials. Data accessed during this intrusion included multiple software products produced by, or licensed to, Zombie Studios. [REDACTED] additionally reviewed a Zombie Studios internal website describing how to connect to a United States Army Perforce server.
- cc. On or about November 27, 2012, [REDACTED] accessed Zombie Studios employee C.L.'s computer. [REDACTED] also had previously accessed C.L.'s Outlook webmail account, and had executed a "forced password reset," which allowed [REDACTED] to use C.L.'s Outlook account to access the United States Army's Perforce

Virtual Private Network. C.L. was authorized to access the United States Army's Perforce Virtual Private Network in connection with Zombie Studios' contract for the design of United States Army Apache Helicopter Pilot simulation software entitled, "AH-64D Apache Simulator."

dd. On or about December 11, 2012, via computers connected to the Internet from Australia, [REDACTED] logged into the United States Army's Perforce Virtual Private Network server using the new password and log-in credentials for C.L.'s account.

ee. During this December 11, 2012 trespass into the United States Army's Perforce Virtual Private Network, [REDACTED] accessed Army Apache Helicopter Pilot simulation software entitled "AH-64D Apache Simulator," which was developed by Zombie Studios under contract with the United States Department of Army.

ff. On or about April 10, 2013, D.W. provided Person A, who was connected to the Internet from Delaware, with access to a server controlled by [REDACTED] and permitted Person A to download approximately five gigabytes of files pertaining to the "AH-64D Apache Simulator."

gg. Zombie Studios maintained a firewall log of "offending" IP addresses, which had attempted or completed unauthorized, remote connections to Zombie Studios' network during the approximate date range of May 2012 through January 2013. Within this period, the following IP addresses, which were known to have been utilized by [REDACTED] to access Zombie Studios' computer network, had the following number of records:

203.59.226.40 - approximately 104 entries;

203.59.226.72 - approximately 13 entries;

203.59.226.73 - approximately 3 entries;

203.59.226.75 - approximately 3 entries.

**Microsoft Game Developer Network Portal**

- hh. In or about 2011 and 2012, Microsoft and its development partners were designing a next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," as well as software to be used with the new Xbox console. Microsoft has not yet released "Xbox One" for commercial distribution.
- ii. Microsoft operated a "Game Developer Network Portal" ("GDNP"), which was an online system allowing prospective developers of games for Microsoft's Xbox and other gaming platforms to access, through an authentication system, pre-release Xbox operating system development tools and software. Microsoft controlled access to the GDNP by, among other methods, imposing licensing and other requirements for authorized users to be registered with Microsoft. In addition, Microsoft administered separate access enclaves within GDNP for more-restricted data.
- jj. Microsoft also provided developers with access to a software platform, known as "PartnerNet," to refine video game creation. Microsoft controlled access to PartnerNet by, among other methods, licensing and providing authorized network users with an "Xbox Development Kit" ("XDK"), which are non-retail units used to access PartnerNet.
- kk. Beginning in or about January 2011, POKORA, [REDACTED] and others engaged in incidents of unauthorized access into Microsoft's computer networks,

including GDNP's protected computer network, during which they stole Log-In Credentials, Personal Data, Confidential and Proprietary Corporate Information, Trade Secrets, Copyrighted Works, and Works Being Prepared for Commercial Distribution relating to the Xbox gaming system. In particular, POKORA, [REDACTED] and others accessed GDNP with valid, but stolen, accounts associated with legitimate Microsoft software-development partners.

- ll. During an online electronic communication session conducted by the co-conspirators via Skype on or about August 11, 2011 from computers connected to the Internet from Australia, Canada, Delaware, and New Jersey, POKORA claimed: "I got a couple of GDN accounts. I actually have over 16,000, just pure developer accounts for different studios."
- mm. In or about July and August 2012, NESHEIWAT, POKORA, and [REDACTED] and others engaged in electronic communications from computers connected to the Internet from Australia, Canada, Maryland, New Jersey, and Delaware, and shared information that they had gained from accessing Microsoft's PartnerNet and GDNP. The co-conspirators then entered email addresses, passwords, and account usernames of Microsoft's Xbox-related development partners they had obtained until they found active accounts that could be used to gain unauthorized access to Microsoft's computer networks. The group then spent hundreds of hours searching through these networks for unprotected files.
- nn. Using the stolen Log-In Credentials that provided them access to Microsoft's computer networks, POKORA, [REDACTED] and LEROUX copied files containing or

relating to the specialized operating system with software source code, technical specifications, assembly instructions, and software design and source code writing specifications for use by game developers for the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.

- oo. LEROUX, POKORA, and [REDACTED] agreed to use this stolen data and operating system software to manufacture and then sell a counterfeit version of the next generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.
- pp. LEROUX subsequently ordered hardware components from NewEgg.com and other online vendors to build a counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.
- qq. During an electronic communication conducted on or about July 24, 2012 via Skype from computers connected to the Internet from Canada, Australia, and Delaware, POKORA, [REDACTED], and Person A discussed a plan pursuant to which Person A would travel from Delaware to LEROUX's residence in Maryland to obtain custody of the counterfeit version of the next-generation Xbox gaming console built by LEROUX.

- rr. Person A was instructed by the co-conspirators to send, by United States Mail, the counterfeit version of the next-generation Xbox gaming console built by LEROUX from Delaware to an individual located in Victoria, Mahe, Republic of Seychelles.
- ss. On or about August 9, 2012, Person A traveled from Delaware to LEROUX's Maryland residence, where LEROUX gave Person A the counterfeit version of the next-generation Xbox gaming console built by LEROUX, with the understanding that Person A would transport the counterfeit Xbox console into Delaware and then mail it to the Republic of Seychelles.
- tt. On or about August 9, 2012, Special Agents of the Federal Bureau of Investigation obtained, from Person A in Delaware, the counterfeit version of the next-generation Xbox gaming console built by LEROUX. Microsoft subsequently confirmed that this counterfeit version of the next-generation Xbox gaming console contained stolen Microsoft intellectual property.
- uu. In or about August 2012, [REDACTED] listed another counterfeit version of the next generation Xbox gaming console for sale on eBay.com. [REDACTED] sold this counterfeit version of the next-generation Xbox gaming console for approximately \$5,000.
- vv. [REDACTED] paid LEROUX a portion of the sales proceeds from the counterfeit version of the next generation Xbox gaming console by giving LEROUX access to D.W.'s credit card.
- ww. On or about February 22, 2013, "Kotaku.com," a website devoted to the discussion of computer games, published an article entitled: "The Rise and

Fall of SuperDaE, a Most Unusual Video Game Hacker." In this article, [REDACTED] was quoted as discussing his unauthorized access to a next-generation Xbox gaming console and his dissemination of approximately 20 Microsoft confidential documents to a person associated with "Kotaku.com."

All in violation of Title 18, United States Code, Section 371.

**COUNT 2**  
**(Conspiracy to Commit Wire Fraud)**  
**18 U.S.C. §§ 1343 & 1349**

6. The allegations contained in paragraphs 1 through 5 of the Indictment are re-alleged and incorporated as if set forth herein.

7. Between in or about January 2011 and April 2013, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefire4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

did knowingly and intentionally conspire and agree among themselves and with others known and unknown to the grand jury, including [REDACTED], C.W., to execute a scheme and artifice to commit wire fraud, in violation of Title 18, United States Code, Section 1343, to wit, devising and intending to devise a scheme and artifice to defraud and to obtain money and property by

means of false and fraudulent pretenses, representations and promises, as set forth in Paragraphs 1 through 5 above, and in furtherance thereof, on or about the dates set forth below, in the District of Delaware and elsewhere, causing to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, namely, Log-In Credentials assigned to actual employees of the Victims, for the purpose of executing such scheme and artifice:

Approximate Dates	Corporate Victims
January 2011-March 2012	Epic Games, Inc.
September 2011-November 2012	Valve Corporation
May 2011-December 2012	Microsoft Corporation
May 2012-April 2013	Zombie Studios/U.S. Army

All in violation of Title 18, United States Code, Sections 1343 and 1349.

**COUNTS 3-6  
(Wire Fraud)  
18 U.S.C. § 1343**

8. The allegations contained in paragraphs 1 through 5 of the Indictment are re-alleged and incorporated as if set forth herein.

9. On or about each of the dates set forth below, each instance constituting a separate count, in the District of Delaware and elsewhere, the defendants,

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,

a/k/a "rampuptechie,"

a/k/a "Soniciso,"

a/k/a "Sonic," and

DAVID POKORA,

a/k/a "Xenomega 9,"

a/k/a "Xenon7,"

a/k/a "Xenomega,"

having intentionally devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, knowingly transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, the following writings, signs, signals, pictures, and sounds:

Count	Approximate Date	Description of Wire Transmission
3	6/2011	Unlawful download from Epic's computer network of pre-release "Gears of War 3" software
4	9/2011	Unlawful download from Valve's computer network of pre-release "Call of Duty: Modern Warfare 3" software
5	8/2011	Unlawful download of Confidential and Proprietary Data of Microsoft Corporation; Trade Secrets and Copyrighted Material relating to the next generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution
6	12/2012	Unlawful download from U.S. Army computer network of "AH-64D Apache Simulator" software

All in violation of Title 18, United States Code, Section 1343.

**COUNT 7**  
**(Conspiracy to Commit Theft of Trade Secrets)**  
**18 U.S.C. §§ 1832(a)(1), (a)(2), (a)(3) & (a)(5)**

10. The allegations contained in paragraphs 1 through 5 of the Indictment are re-alleged and incorporated as if set forth herein.

11. Between in or about January 2011 and in or about February 2013, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "conféttimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

with the intent to convert a Trade Secret to the economic benefit of someone other than its owner, did knowingly and intentionally conspire and agree among themselves and with others known and unknown to the grand jury, including [REDACTED] C.W., to commit theft of trade secrets, in violation of Title 18, United States Code, Sections 1832(a)(1), (a)(2), (a)(3) and (a)(5), to wit, to steal, and without authorization appropriate, take, carry away, copy, duplicate, download, upload, replicate, transmit, deliver, send, mail, communicate, convey and possess Trade Secrets owned by Microsoft Corporation, that is, Xbox Gaming System technology, including the specialized operating system with software source code, technical specifications, descriptions of expected performance characteristics, plans for the development of new features, descriptions of

assembly instructions, descriptions of processing unit functionality, and software design and source code writing specifications for use by game developers for the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," and which is related to and included in a product that is produced for and placed in interstate and foreign commerce, knowing that the Trade Secrets had been stolen, appropriated, obtained, and converted without authorization, and intending and knowing that the disclosure would injure Microsoft.

**MANNER AND MEANS OF THE CONSPIRACY**

12. The manner and means by which LEROUX, NESHEIWAT, POKORA, [REDACTED], and their co-conspirators sought to accomplish the conspiracy included, among other things, the following:

- a. It was part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would unlawfully obtain authentic Log-In Credentials for Microsoft's Game Development Network Portal ("GDNP").
- b. It was further part of the conspiracy that POKORA and [REDACTED] would gain unauthorized access to Microsoft's GDNP using the stolen Log-In Credentials and would download Microsoft Copyrighted Works, Works Being Prepared for Commercial Distribution, and Trade Secrets relating to the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," and which was being prepared for commercial distribution.
- c. It was further part of the conspiracy that POKORA and [REDACTED] would share copies of the stolen Microsoft Trade Secrets with co-conspirators in an effort to build

and then sell a counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.

- d. It was further part of the conspiracy that the co-conspirators would share the proceeds from the sale of the counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.

#### OVERT ACTS

13. In furtherance of the conspiracy, the following overt acts, among others, were committed in the District of Delaware and elsewhere:

- a. In or about 2011 and 2012, Microsoft and its development partners were designing a next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One," as well as software to be used with the new Xbox console. Microsoft has not yet released "Xbox One" for commercial distribution.
- b. Beginning in or about January 2011, POKORA, [REDACTED] and others engaged in incidents of unauthorized access into Microsoft's computer networks, including Microsoft's "Game Developer Network Portal" ("GDNP"), during which they stole Log-In Credentials, Trade Secrets, and Intellectual Property relating to the Xbox gaming system. In particular, POKORA, [REDACTED] and others accessed GDNP with valid, but stolen, accounts associated with legitimate Microsoft software-development partners.

- c. During an online electronic communication session conducted via Skype on or about August 11, 2011 from computers connected to the Internet from Australia, Canada, Delaware, and New Jersey, POKORA claimed: "I got a couple of GDN accounts. I actually have over 16,000, just pure developer accounts for different studios."
- d. In or about July and August 2012, NESHEIWAT, POKORA, and [REDACTED] and others engaged in electronic communications from computers connected to the Internet from Australia, Canada, Maryland, New Jersey, and Delaware, and shared information that they had gained from accessing Microsoft's PartnerNet and GDNP. The co-conspirators then entered email addresses, passwords, and account usernames of Microsoft's Xbox-related development partners they had obtained until they found active accounts that could be used to gain unauthorized access to Microsoft's computer networks. The group then spent hundreds of hours searching through these networks for unprotected files.
- e. Using the stolen Log-In Credentials that provided them access to Microsoft's computer networks, POKORA, [REDACTED] and LEROUX copied files containing or relating to the specialized operating system with software source code, technical specifications, assembly instructions, and software design and source code writing specifications for use by game developers for the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.
- f. LEROUX, POKORA, and [REDACTED] agreed to use this stolen data and operating system software to manufacture and then sell a counterfeit version of the next

generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.

- g. LEROUX subsequently ordered components from "NewEgg.com" and other online vendors to build a counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution.
- h. During an electronic communication conducted on or about July 24, 2012 via Skype from computers connected to the Internet from Canada, Australia, and Delaware, POKORA, [REDACTED] and Person A discussed a plan pursuant to which Person A would travel from Delaware to LEROUX's residence in Maryland to obtain custody of the counterfeit version of the next-generation Xbox gaming console built by LEROUX.
- i. Person A was instructed by the co-conspirators to send, by United States Mail, the counterfeit version of the next-generation Xbox gaming console built by LEROUX from Delaware to an individual located in Victoria, Mahe, Republic of Seychelles.
- j. On or about August 9, 2012, Person A traveled from Delaware to LEROUX's Maryland residence, where LEROUX gave Person A the counterfeit version of the next-generation Xbox gaming console built by LEROUX, with the understanding that Person A would transport the counterfeit version of the next generation Xbox gaming console into Delaware and then mail it to the Republic of Seychelles.

- k. On or about August 9, 2012, Special Agents of the Federal Bureau of Investigation obtained the counterfeit version of the next-generation Xbox gaming console built by LEROUX from Person A in Delaware. Microsoft subsequently confirmed that this counterfeit version of the next-generation Xbox gaming console contained stolen Microsoft intellectual property.
- l. In or about August 2012, [REDACTED] listed another counterfeit version of the next generation Xbox gaming console for sale on eBay.com. [REDACTED] sold the counterfeit version of the next-generation Xbox gaming console for approximately \$5,000.
- m. [REDACTED] paid LEROUX a portion of the sales proceeds from the counterfeit version of the next-generation Xbox gaming console by giving LEROUX access to [REDACTED]'s credit card.
- n. On or about February 22, 2013, "Kotaku.com," a website devoted to the discussion of computer games, published an article entitled: "The Rise and Fall of SuperDaE, a Most Unusual Video Game Hacker." In this article, [REDACTED] was quoted as discussing his unauthorized access to a next-generation Xbox gaming console and his dissemination of approximately 20 Microsoft confidential documents to a person associated with "Kotaku.com."

All in violation of Title 18, United States Code, Sections 1832(a)(1), (a)(2), (a)(3) and (a)(5).

**COUNTS 8-10**  
**(Unauthorized Computer Access)**  
**18 U.S.C. § 1030(a)(2)(C) & 2**

14. The allegations contained in paragraphs 1 through 13 of the Indictment are re-alleged and incorporated as if set forth herein.

15. Between in or about January 2011 and in or about December 2012, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

and others known and unknown to the grand jury, intentionally accessed a protected computer without authorization for purposes of commercial advantage and private financial gain and to obtain information, as set forth below, the value of which exceeded \$5,000, from a protected computer:

Count	Approximate Date	Amount of Value Obtained
8	January 2011- March 2012	Confidential and Proprietary Data of Epic Games, Inc.; Pre-Release Copy of "Gears of War 3" Software
9	September 2011- November 2012	Confidential and Proprietary Data of Valve Corporation; Pre-Release Copy of "Call of Duty: Modern Warfare 3" Software
10	May 2011- December 2012	Confidential and Proprietary Data of Microsoft Corporation; Trade Secrets and Copyrighted Material relating to the next generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution

All in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(i) and (iii) & 2.

**COUNT 11**  
**(Criminal Copyright Infringement)**  
**17 U.S.C. § 506(a)(1)(C) & 18 U.S.C. § 2319(d)(2) & 2**

16. Paragraphs 1-13 are re-alleged and incorporated as if set forth herein.

17. Between in or about January 2011 and in or about July 2011, in the District of Delaware and elsewhere, the defendants,

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

and others known and unknown to the grand jury, did willfully, for the purpose of commercial advantage and private financial gain, infringe a copyright by the distribution of the Copyrighted Work listed below being prepared for commercial distribution by making the work available on a computer network accessible to members of the public, when the defendants knew and should have known that the work was intended for commercial distribution:

Count	Copyrighted Work	Pre-Release Work Infringed
11	Epic Games & Microsoft Corporation	Pre-Release Copy of "Gears of War 3" Software

All in violation of Title 17, United States Code, Section 506(a)(1)(C) and Title 18, United States Code, Section 2319(d)(2) & 2.

**COUNT 12**  
**(Criminal Copyright Infringement)**  
**17 U.S.C. § 506(a)(1)(C) & 18 U.S.C. § 2319(d)(2) & 2**

18. Paragraphs 1-13 are re-alleged and incorporated as if set forth herein.

19. Between in or about January 2011 and in or about July 2011, in the District of Delaware and elsewhere, the defendants,

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

and others known and unknown to the grand jury, did willfully, for the purpose of commercial advantage and private financial gain, infringe a copyright by the distribution of the Copyrighted Work listed below being prepared for commercial distribution by making the work available on a computer network accessible to members of the public, when the defendants knew and should have known that the work was intended for commercial distribution:

Count	Copyright Holder(s)	Pre-Release Work Infringed
12	Activision Blizzard, Inc.	Pre-Release Copy of "Call of Duty: Modern Warfare 3" Software

All in violation of Title 17, United States Code, Section 506(a)(1)(C) and Title 18, United States Code, Section 2319(d)(1) & (2) & 2.

**COUNT 13**  
**(Conspiracy to Commit Mail Fraud)**  
**18 U.S.C. §§ 1341 & 1349**

20. The allegations contained in paragraphs 1-13 of the Indictment are re-alleged and incorporated as if set forth herein.

21. Between in or about August 2011 and in or about August 2012, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefire4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

did knowingly and intentionally conspire and agree among themselves and with others known and unknown to the grand jury, including [REDACTED] C.W., to execute a scheme and artifice to commit mail fraud, in violation of Title 18, United States Code, Section 1341, to wit, devising and intending to devise a scheme and artifice to defraud and obtain money by materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute the above-described scheme and artifice to defraud, the defendants knowingly caused to be delivered by mail at the place at which it was directed to be delivered by the person to whom it was addressed, to wit, an individual located in Victoria, Mahe, Republic of Seychelles, the following matter: a counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution,

All in violation of 18 U.S.C. §§ 1341 and 1349.

**COUNT 14**  
**(Attempted Mail Fraud)**  
**18 U.S.C. § 1341**

22. The allegations contained in paragraphs 1 through 13 of the Indictment are re-alleged and incorporated as if set forth herein.

23. Between in or about August 2011 and in or about August 2012, in the District of Delaware and elsewhere, the defendant

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

did knowingly and intentionally devise a scheme and artifice to defraud and obtain money by materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute the above-described scheme and artifice to defraud, the defendant attempted to cause to be delivered by mail at the place at which it was directed to be delivered by the person to whom it was addressed, to wit, an individual located in Victoria, Mahe, Republic of Seychelles, the following matter: a counterfeit version of the next-generation Xbox gaming console, which Microsoft internally codenamed "Durango" and later publicly named "Xbox One" and which was being prepared for commercial distribution,

All in violation of 18 U.S.C. § 1341.

**COUNT 15**  
**(Conspiracy to Commit Identity Theft)**  
**18 U.S.C. § 1028(f)**

24. The allegations contained in paragraphs 1 through 13 of the Indictment are re-alleged and incorporated as if set forth herein.

25. Between in or about January 2011 and in or about February 2013, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

did knowingly and intentionally conspire and agree among themselves and with others known and unknown to the grand jury, including [REDACTED] and C.W., to commit identity theft, in violation of Title 18, United States Code, Section 1028(a)(7) and (b)(1), to wit, transferring, possessing, and using, without lawful authority, in a manner affecting interstate commerce, means of identification of other persons with the intent to commit, and to aid and abet, and in connection with, unlawful activity, namely: (1) conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349; (2) conspiracy to commit theft of trade secrets, in violation of Title 18, United States Code, Sections 1832(a)(1), (a)(2), (a)(3), and (a)(5); and (3) criminal copyright infringement, in violation of Title 18, United States Code, Section 2319(d)(2).

**MANNER AND MEANS OF THE CONSPIRACY**

26. The manner and means by which LEROUX, NESHEIWAT, POKORA, [REDACTED] and others sought to accomplish the conspiracy included, among other things, the following:

- a. It was part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would visit websites where another hacker had posted legitimate Log-In Credentials for persons who were authorized to access certain computer networks, and would copy those Log-In Credentials and save them for subsequent use.
- b. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would conduct computer network reconnaissance for the purpose of finding and stealing Log-In Credentials.
- c. It was further part of the conspiracy that LEROUX, NESHEIWAT, POKORA, and [REDACTED] would use the stolen Log-In Credentials to gain unauthorized access to Victims' computer networks to steal additional Log-In Credentials, Personal Data, Authentication Keys, Corporate Documents, Card Data, Trade Secrets, Copyrighted Works, and Works Being Prepared For Commercial Distribution.

#### OVERT ACTS

27. In furtherance of the conspiracy, the following overt acts, among others, were committed in the District of Delaware and elsewhere:

28. In or about January 2011, POKORA used legitimate Log-In Credentials of another person to gain unauthorized access to Epic's computer network, and to copy and download Epic's Copyrighted Works and Works Being Prepared For Commercial Distribution, including the game "Gears of War 3."

29. In or about June 2011, [REDACTED] used legitimate Log-In Credentials of another person to gain unauthorized access to Epic's computer network, and to copy a legal document belonging to Epic and marked "Attorney-Client Privileged" to a computer controlled by [REDACTED]

30. In or about June 2011, NESHEIWAT used legitimate Log-In Credentials of another person to gain unauthorized access to Epic's computer network, and to copy and download Epic's Copyrighted Works and Works Being Prepared For Commercial Distribution, including "Gears of War 3" gaming software.

31. During an online electronic communication session that was conducted on or about August 11, 2011 via Skype and accessed from computers connecting to it from Australia, Canada, Delaware, and New Jersey, POKORA claimed: "I got a couple of GDN accounts. I actually have over 16,000, just pure developer accounts for different studios."

32. On or about September 28, 2011, POKORA obtained legitimate Log-In Credentials of another person for Valve's computer network, and provided online access to these Log-In Credentials to Person A, who was connected to the Internet from a computer located in Delaware. POKORA also used these Log-In Credentials to gain unauthorized access to Valve's computer network, and to download a file containing Works Being Prepared For Commercial Distribution, including the game "Call of Duty: Modern Warfare 3."

33. On or about September 28, 2011, via electronic communications transmitted to computers connecting to the Internet from, among other places, Delaware, New Jersey, Maryland and Canada, POKORA, his co-conspirators and Person A utilized TeamViewer software to jointly and remotely access a computer controlled by POKORA. This computer contained multiple databases within a "Hacking" folder, labeled in a manner consistent with the Victims' names, including: Epic Games (i.e., "epicgames\_user\_db\_cracked") and Valve Corp. (i.e., "steam\_valve\_accs.html"). POKORA provided Person A with access to these databases, which contained compromised means of identification for over 200 individual victim accounts and included fields such as username, password, and e-mail addresses. POKORA also provided

access to usernames, passwords, encrypted passwords or "password hashes," and e-mail addresses, for approximately 47 additional accounts.

34. During multiple online electronic communication sessions conducted via Skype on or about July 24, 2012, and accessed from computers connecting to the Internet from Australia, Canada, Maryland, New Jersey, and Delaware, POKORA and [REDACTED] provided members of the conspiracy with legitimate Log-In Credentials for Microsoft's "Game Development Network Portal" computer network.

35. On or about July 29, 2012, via computers connected to the Internet from, among other places, Delaware, Maryland, Australia and Canada, [REDACTED] LEROUX and others, including Person A, utilized stolen Log-In Credentials to access the computer network of Zombie Studios.

36. During this intrusion, [REDACTED] accessed pre-release software and software builds for gaming software being developed by Zombie Studios, as well as personally identifying information of Zombie Studios' employees. [REDACTED] transmitted the means of identification, including the name, social security number, home address, and tax documents, of "C.L.," a Zombie Studios employee, to Person A in Delaware. After gaining access to C.L.'s Personal Data, [REDACTED] subsequently submitted credit card applications in the names of C.L. and M.L., for limits of \$15,000 and \$10,000. [REDACTED] additionally attempted to open a "Lendingclub.com" account in the name of C.L. for approximately \$20,000. [REDACTED] accessed these accounts online and provided a Delaware mailing address associated with Person A to defeat financial institution anti-fraud countermeasures.

37. Person A subsequently received credit account activation notices in the names of C.L. and M.L. via United States Mail, at a Delaware address.

38. On or about February 20, 2013, Person A, while located in Delaware, received a database file named "db.html," which contained approximately 11,621 stolen Log-In Credentials for victim computer networks that had been assembled by members of the conspiracy.

All in violation of Title 18, United States Code, Section 1028(f).

**COUNT 10** *Sum 7/23/13*  
**(Aggravated Identity Theft)**  
**18 U.S.C. § 1028A & 2**

39. The allegations contained in paragraphs 1 through 38 of the Indictment are re-alleged and incorporated as if set forth herein.

40. In or about October 2011, in the District of Delaware and elsewhere, the defendants

NATHAN LEROUX,  
a/k/a "natelx,"  
a/k/a "animefre4k,"  
a/k/a "confettimancer,"  
a/k/a "void mage,"  
a/k/a "Durango,"  
a/k/a "Cthulhu,"

SANADODEH NESHEIWAT,  
a/k/a "rampuptechie,"  
a/k/a "Soniciso,"  
a/k/a "Sonic," and

DAVID POKORA,  
a/k/a "Xenomega 9,"  
a/k/a "Xenon7,"  
a/k/a "Xenomega,"

did knowingly transfer, possess, and use, without lawful authority, means of identification of another person, including but not limited to Log-In Credentials belonging to W.E., an employee of Epic Games, during and in relation to a conspiracy to commit wire fraud and wire fraud, as alleged in Counts 2 and 3-6, in violation of Title 18, United States Code, Section 1028A & 2.

**NOTICE OF FORFEITURE**

41. As a result of the offenses alleged in Counts 1 and 8-10 of this Indictment, the defendants POKORA, LEROUX and NESHEIWAT shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 1030(i) and 1030(j), any interest in any personal property that was used and intended to be used to commit and to facilitate the commission of the criminal violations charged in Counts 1 and 8-10 of this Indictment, and any property, real and personal, constituting and derived from, any proceeds that any defendant obtained, directly and indirectly, as a result of such violations.

42. As a result of the offenses alleged in Counts 1, 11 and 12 of this Indictment, the defendants POKORA, LEROUX and NESHEIWAT shall forfeit to the United States, pursuant to Title 17, United States Code, Sections 506(b) and 509(a), and Title 18 United States Code, Section 2323, all copies manufactured, reproduced, distributed, sold, or otherwise used, intended for use, or possessed with intent to use in violation of the offense under Section 506(a), and all plates, molds, matrices, masters, tapes, film negatives, or other articles by means of which such copies may be reproduced, and all electronic, mechanical, and other devices for manufacturing, reproducing, and assembling such copies, and any property used, or intended to be used in any manner or part, to commit or facilitate the commission of the offenses in Counts 1, 11 and 12.

43. Furthermore, upon conviction of an offense alleged in Counts 1, 11 and 12 of this Indictment, the defendants POKORA, LEROUX and NESHEIWAT shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 17 U.S.C. § 506(a)(1)(C) and 18 U.S.C. § 2319.

44. Upon conviction of the offenses alleged in Counts 15 and 16 of this Indictment, the defendants POKORA, LEROUX and NESHEIWAT shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1028(b)(5) and (g) and Title 21, United States

Code, Section 853, any personal property that was used or intended to be used in the commission of the offenses charged in Counts 15 and 16.

45. Upon conviction of the offenses alleged in Counts 1-2, 3-6, 14-15 of this Indictment, the defendants POKORA, LEROUX and NESHEIWAT shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses.

46. The personal property that is subject to forfeiture pursuant to Paragraphs 39-43 includes, but is not limited to the following:

- a. GATEWAY SERVER S/N G1436120044
- b. CUSTOM BUILT PC S/N CA14810022770
- c. CUSTOM BUILT PC, NO S/N, NO SIDE COVERS
- d. HP DESKTOP S/N MXX4480RIY
- e. 8 MB MEMORY CARD NO S/N
- f. T-MOBILE CELL HT848G722446
- g. SAMSUNG CELL S/N 268435461700346534 - NO BACK COVER
- h. IPHONE NO S/N - BACK COVER REMOVED
- i. NOKIA CELL S/N 357617/00/646480 WITH POWER
- j. SAMSUNG CELL S/N 014150638080EE5DB00
- k. PALM CELL S/N P5PE077954TT
- l. LG CELL S/N 906KPTM322033
- m. LG CELL S/N 011KPRW0290262
- n. XBOX 360 S/N 124988374507 (NO CASE)

- o. DESKTOP COMPUTER S/N 83-102-685
- p. XBOX 360 WITH ADAPTER S/N 008016680907 (NO CASE)
- q. XBOX 360 WITH ADAPTER S/N 000L20671507
- r. GATEWAY LAPTOP S/N P248391018104
- s. TOSHIBA HD PARTIAL S/N 695QH
- t. TOSHIBA HD 40A8P56HT
- u. NDEV BOX WITH CABLES S/N NMA200110264
- v. SEAGATE HDD S/N 5QF11VEM
- w. TOSHIBA HDD S/N 40MES72HS
- x. MOTOROLA CABLE MODEM S/N 0J34TW5YM0V4
- y. CABLE MODEM S/N 9451J23001070 (PLUGGED IN)
- z. NINTENDO WEIU S/N GW10066372
- aa. SEAGATE EXT S/N 2GETAVMS
- bb. SEAGATE EXT HDD S/N 2GHHB987
- cc. WESTERN DIGITAL HDD S/N WX91AA0R3537
- dd. SAMSUNG HDD S/N S2H7J9EZC09856
- ee. HITACHI HDD S/N 120603EZ0153412EUBEJ
- ff. FUJITSU HDD S/N K60L5892AP5R
- gg. TOSHIBA HDD S/N 692BT2N7T
- hh. COMPAQ S/N 1V0AFP4DM158
- ii. MACBOOK S/N W8925DZA9GU
- jj. IBM LAPTOP S/N 60RK011
- kk. GATEWAY S/N 0029904687

ll. GATEWAY S/N N3456C1023867  
mm. COMPAQ PRESARIO S/N 2CE918C24G  
nn. XBOX 360 S/N 518295573205  
oo. XBOX 360 S/N 601486374605 WITH ADAPTER  
pp. XBOX 360 S/N 300500671505  
qq. XBOX 360 S/N 800162461206  
rr. SONY PLAYSTATION 2 S/N 600991  
ss. SONY PS3 S/N 00-27450252-0201153-DECR-1400A  
tt. SONY PS3 (RED) NO S/N  
uu. PLAYSTATION S/N 354162 WITH NETWORK ADAPTER  
vv. XBOX S/N X0153-500  
ww. XBOX 360 S/N D711CG920801000JK  
xx. NINTENDO GAME CUBE S/N NRR 04901  
yy. MICROSOFT XBOX S/N 311233122202, NO CASE  
zz. NINTENDO 64 S/N N513705912Y  
aaa. Hitachi 120 GB hard drive  
bbb. Nikon D5000 Digital camera s/n 3491648  
ccc. Wii s/n LU96455396-3  
ddd. XBox 360 s/n 163443783505 labeled: lobby box 9000  
eee. XBox 360 s/n 070685273207  
fff. XBox 360 s/n 449267320405  
ggg. Playstation 2 , PT235488000, s/n U3548800  
hhh. Black Sony PS3 s/n CF557720444-CECH-3001B

iii. MacBook Pro s/n c02J1F5WDKQ1 and MagSafe Power Adapter

jjj. XBox Kinect serial #166998312905

kkk. Dell computer s/n SQ41Pm1 / service tag 6Q41PM1

47. If any of the property described above, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p) (as incorporated by Title 18, United States Code, Section 982(b)(1) and Title 28, United States Code, Section 2461(o)).

A TRUE BILL:



CHARLES M. OBERLY, III  
UNITED STATES ATTORNEY

A handwritten signature in black ink, appearing to read "Ed McAndrew", written over a horizontal line.

Edward J. McAndrew  
Assistant United States Attorney

MYTHILI RAMAN  
ACTING ASSISTANT ATTORNEY GENERAL  
U.S. DEPARTMENT OF JUSTICE, CRIMINAL DIVISION

A handwritten signature in black ink, appearing to read "James Silver", written over a horizontal line.

James Silver  
Trial Attorney, Computer Crime & Intellectual Property Section

Dated: July 23, 2013